UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE: CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION	)	MDL No. 1:19-md-02915 (AJT-JFA)

This Document Relates to the Consumer Cases

MEMORANDUM OF LAW IN SUPPORT OF
AMAZON'S MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

Page

TABLE OF CONTENTS
(Continued)

Page

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(Continued)

Page(s)

TABLE OF AUTHORITIES
(Continued)

Page(s)

TABLE OF AUTHORITIES
(Continued)

Page(s)

TABLE OF AUTHORITIES
(Continued)

Page(s)

STATUTES AND RULES

TABLE OF AUTHORITIES
(Continued)

Page(s)

OTHER AUTHORITIES

TABLE OF EXHIBITS

No.	Exhibit
1	Excerpted Transcript of the Deposition of Capital One 30(b)(6) Witness Michael Fisk, taken on May 15, 2020
2	Excerpted Transcript of the Deposition of Capital One 30(b)(6) Witness David Thomas Frei, taken on June 9, 2020
3	Excerpted Transcript of the Deposition of Capital One 30(b)(6) Witness Mark Donovan, taken on October 14, 2020
4	Excerpted Transcript of the Deposition of Biba Helou, taken on October 8, 2020
5	Excerpted Transcript of the Deposition of Houston Hopkins, taken on October 15, 2020
6	Excerpted Transcript of the Deposition Capital One 30(b)(6) Witness Heather Caputo, taken on September 25, 2020
7	Excerpted Transcript of the Deposition of Michael Hedrick, taken on October 26, 2020
8	Excerpted Transcript of the Deposition of Capital One 30(b)(6) Witness Diane Lye, taken on June 3, 2020
9	Excerpted Transcript of the Deposition of Robert Alexander, taken on August 28, 2020
10	Excerpted Transcript of the Deposition of Capital One 30(b)(6) Witness Jack Walker, taken on July 16, 2020
11	Excerpted Transcript of the Deposition of Capital One 30(b)(6) Witness Terren Peterson, taken on May 20, 2020
12	Excerpted Transcript of the Deposition of Christopher Schultz, taken on September 9, 2020
13	Excerpted Transcript of Mandiant witness DJ Palombo, taken on November 16, 2020
14	Biba Helou Deposition Exhibit 230

No.	Exhibit
15	Houston Hopkins Deposition Exhibit 279
16	Michael Hedrick Deposition Exhibit 352
17	Robert Alexander Deposition Exhibit 31
18	Robert Alexander Deposition Exhibit 32
19	Christopher Schultz Deposition Exhibit 80
20	DJ Palombo Deposition Exhibit 761
21*[1]	Capital One Defendants' March 5, 2021 Supplemental Responses to Interrogatories Nos. 10, 11, 13, and 14
22*	Capital One Defendants' June 9, 2020 Supplemental Response to Interrogatory No. 7
23*	Capital One Defendants' March 12, 2020 Amended Response to Interrogatory No. 20
24	Excerpted Transcript of the Deposition of AWS 30(b)(6) Witness Michael Haken, taken on June 9, 2020
25	Excerpted Transcript of the Deposition of AWS 30(b)(6) Witness Steve Schuster, taken on June 11, 2020
26	Excerpted Transcript of the Deposition of Stephen Schmidt, taken on September 18, 2020
27	Excerpted Transcript of the Deposition of AWS 30(b)(6) Witness Stephen Schmidt, taken on January 8, 2021
28	Excerpted Transcript of the Deposition of Don Barber, taken on September 22, 2020

[1] Exhibits further supported by the attached Declaration of Tyler Newby in support of Amazon's Motion for Summary Judgment.

No.	Exhibit
29	Excerpted Transcript of the Deposition of AWS 30(b)(6) Witness Brian Bentzen, taken on November 17, 2020
30	Don Barber Deposition Exhibit 140
31	Brian Bentzen 30(b)(6) Deposition Exhibit 773
32	Brian Bentzen 30(b)(6) Deposition Exhibit 768
33	Brian Bentzen 30(b)(6) Deposition Exhibit 769
34*	AWS_CAP00001271
35*	AWS_CAP00000018–19
36*	AWS_CAP00001212–1214
37*	AWS_CAP00001247–1250
38*	AWS_CAP00001231–1240
39*	AWS_CAP00002976
40*	AWS_CAP00002603
41*	AWS_CAP00001209
42*	AWS_CAP00001215
43*	AWS_CAP00001217
44*	AWS_CAP00001222
45*	AWS_CAP00002698
46*	Expert Rebuttal Report of Don Good

No.	Exhibit
47*	Microsoft Azure: Shared Responsibility in the Cloud
48	Excerpted Transcript of the Deposition of Plaintiffs' Expert Witness Stuart E. Madnick, taken on June 9, 2021
49	Excerpted Transcript of the Deposition of Representative Plaintiff Emily Behar, taken on July 17, 2020
50	Excerpted Transcript of the Deposition of Representative Plaintiff Brandi Edmondson, taken on November 13, 2020
51*	CAPITALONE_MDL_002204709
52	Excerpted Transcript of the Deposition of Representative Plaintiff Emily Gershen, taken on June 10, 2020
53	Excerpted Transcript of the Deposition of Representative Plaintiff Brandon Hausauer, taken on June 16, 2020
54	Excerpted Transcript of the Deposition of Representative Plaintiff Sara Sharp, taken on June 25, 2020
55	Excerpted Transcript of the Deposition of Representative Plaintiff John Spacek, taken on July 14, 2020
56	Excerpted Transcript of the Deposition of Representative Plaintiff Caralyn Tada, taken on July 8, 2020
57	Excerpted Transcript of the Deposition of Representative Plaintiff Gary Zielicke, taken on May 28, 2020

INTRODUCTION

After more than a year of discovery, Plaintiffs are unable to come forward with any facts to support their claims that Amazon is responsible for a criminal hacker's theft of varied data about Capital One credit cardholders and applicants (the "Cyber Incident"). To the contrary, the undisputed facts show that the Cyber Incident took place only as the result of a unique combination of configurations that were exclusively under the control of Capital One without the knowledge or involvement of Amazon. Additionally, as Capital One establishes in its motion for summary judgment (Dkt. 1463), there is no evidence that any cardholder or applicant was harmed as a result of the Cyber Incident. Nor is there any risk of such harm in the future, because law enforcement recovered the data when it arrested the hacker who perpetrated the Cyber Incident.

Amazon is entitled to summary judgment on each of Plaintiffs' remaining claims against it for the following reasons: First, Plaintiffs' negligence claim (Count 1) fails because the facts are clear that Amazon had no legal duty to Plaintiffs to protect their PII from a third party hacker and that Amazon did not proximately cause any injury to Plaintiffs. Second, Plaintiffs' unjust enrichment claim (Count 3) fails because the facts are undisputed that Plaintiffs did not provide any benefit to Amazon, and that Amazon did not reasonably expect to pay Plaintiffs for Capital One's use of Amazon Web Services (AWS) cloud computing services. Third, Plaintiffs' state statutory claims (Counts 8–15) all fail because Plaintiffs admittedly did not see or rely on any unidentified, misleading statements by Amazon. Finally, Plaintiffs' declaratory judgment claim (Count 4) fails for the same reasons their substantive claims fail.[2] Now that the factual record has

[2] Amazon adopts and incorporates Capital One's motion for summary judgment on Plaintiffs' declaratory judgment and injunctive relief claims. Dkt. 1463 at 47–49.

been fully developed through extensive discovery, Plaintiffs' claims against AWS fail as a matter of law.

STATEMENT OF UNDISPUTED MATERIAL FACTS

A. Capital One's Migration of Its Information Technology to AWS.

1. In 2015, Capital One began migrating its information technology and data from its on-premises data centers to AWS's cloud computing services. Capital One began the migration to "modernize [its] technology infrastructure." *See* Ex. 9 (Alexander, Capital One 30(b)(6) Tr.) at 15:14–20.

2. Capital One migrated to the cloud in part because it believes that it can operate more securely in the cloud than it could in its own on-premises facilities. *See id.* at 23: 2–17 (testifying regarding Capital One's "view on cybersecurity in the AWS cloud").

3. AWS's provision of cloud computing services to Capital One, and Capital One's payment for those services, are governed by agreements between Capital One and Amazon first entered in [redacted] *See* Ex. 29 (Bentzen, AWS 30(b)(6) Tr.) at 27:15–28:4. Capital One uses [redacted] *See* Ex. 29 (Bentzen 30(b)(6)); Ex. 31 (Bentzen 30(b)(6) Ex. 773).

4. The agreements between Capital One and AWS (the "Contracts") [redacted] *See* Ex. 33 (2015 Enterprise Agreement) ¶ 3.6; Ex. 32 (2019 Enterprise Agreement) ¶ 3.6.

5. Amazon does not use or monetize the data Capital One stores in its AWS accounts. Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 108:5–12 [redacted] *see also* Ex. 29 (Bentzen, AWS 30(b)(6) Tr.) at 26:1–12 ("Q: Does Amazon obtain or use consumer data from Capital One? A: No.").

B. Amazon's Shared Responsibility Model for Security.

6. AWS and its customers, including Capital One, operate under what is known as a "Shared Responsibility" model for security, "where AWS is responsible for the security of the cloud and customers are responsible for security in the cloud." *See* Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 57:2–20; Ex. 34 (AWS_CAP00001271); *see also* Ex. 32 (2019 Enterprise Agreement) Section 4 at 15–16.

7. Under the shared responsibility model, AWS is responsible for securing "the host operating systems and virtualization layer, the physical infrastructure; and customers manage all of their resources, including guest operating systems, storage, identity and access management configuration, all of these services that are configurable as customers […] they are responsible for securing in the cloud." Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 57:2–20; *see also* Ex. 2 (Frei, Capital One 30(b)(6) Tr.) at 54:9–55:10 (stating, "Capital One has management of the majority of the control environment that includes your governance, your operations and the layered security tiers that are above what we call the hypervisor layer, and AWS has management of below the hypervisor layer, which essentially is the physical hardware and their data center with its environmental control"); Ex. 30 (Barber Ex. 140).

8. Amazon's Elastic Cloud Compute (EC2) service is an Infrastructure as a Service (IaaS) in which the customer performs "all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance." Ex. 34 (AWS_CAP00001271). An EC2 "instance" is a virtual computer server that runs on AWS and

that a customer configures for its own purposes. *See* Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 125:13–126:14.

9. AWS customers may store data in S3 buckets, which are data storage systems on AWS. Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 126:1–127:2.

10. AWS does not have "access to the customers' machines nor their configuration or data." *See* Ex. 26 (Schmidt Tr.) at 132:9–14; *see also* Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 129:9–24 (stating that AWS has "built our infrastructure so that we cannot access a guest operating system of our customers' virtual machines" and that AWS does not know "what the configuration and the purpose of that virtual machine might be," nor "its purpose for being [which] would make it impossible for us to understand the configuration and the security implications"); Ex. 25 (Schuster, AWS 30(b)(6) Tr.) at 116:2–20 ("Only the customers could determine whether those [WAFs] were configured appropriately or inappropriately for their use case.").

11. AWS's customers, by design, expect privacy around the customers' own sensitive and proprietary information, and by design Amazon does not access customer data or applications in AWS. *See* Ex. 25 (Schuster, AWS 30(b)(6) Tr.) at 54:2–9 ("Our customers do not want us understanding and knowing the type of data that they're putting into our environment.").

12. Other public cloud IaaS providers—Microsoft Azure and Google Cloud Platform, for example—also follow a shared responsibility model for security. *See* Ex. 46 (Expert Rebuttal Declaration of Donald Good, April 7, 2021 ("Good Rep.")) at 12; *see also* Ex. 47 (Microsoft Azure: Shared responsibility in the cloud).

13. Plaintiffs' technical expert did not identify an industry standard of care for security for providers of IaaS cloud services. *See* Ex. 48 (Madnick Tr.) at 190:6–191:14; *see also* Amazon's Motion to Exclude Testimony of Stuart E. Madnick ("Madnick Daubert Mot.") § II.

C. AWS Provides Security Guidance and Tools to Customers.

14. Amazon provides an Identity and Access Management (IAM) feature to AWS customers that allows customers to manage and restrict the authentication and authorization to AWS resources in their accounts. AWS customers configure IAM to allow or deny access to AWS services and resources. An IAM role is an identity that has certain customer-configured permissions. Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 30:10–31:25; Ex. 35 (AWS_CAP00000018–19); Ex. 36 (AWS_CAP00001212–1214); Ex. 37 (AWS_CAP00001247–1250).

15. Amazon provides numerous guides to customers on best practices for securing their AWS accounts. These include guides and white papers on AWS Security Best Practices (Ex. 39 (AWS_CAP00002976)); Overview of Security Processes (Ex. 40 (AWS_CAP00002603)); documentation on using IAM to restrict access to AWS resources in the customer's accounts (Ex. 41 (AWS_CAP00001209), Ex. 36 (AWS_CAP00001212), Ex. 42 (AWS_CAP00001215), Ex. 43 (AWS_CAP00001217), Ex. 44 (AWS_CAP00001222), Ex. 38 (AWS_CAP00001231)); and how to use a Web Application Firewall developed and offered by AWS to mitigate application vulnerabilities, including security misconfigurations and forgery attacks (Ex. 45 (AWS_CAP00002698)).

16. AWS's publicly posted EC2 User Guide recommends that the customer define the IAM role by attaching permissions to the role for the actions and resources specific to that role through security credentials the customer creates for the role. Ex. 38 (AWS00001231–1240) at 3–4; *see* Dkt. 1249 (Madnick Rep.) at 19. AWS provides guidance to all of its customers on its publicly posted User Guide, advising them that an application running on an EC2 instance retrieves security credentials provided by a role (a set of user-configured permissions) from the instance metadata service. *See id.* Amazon's guidance warns customers not to expose security credentials when using the instance metadata service with IAM roles. *Id.*

17. Capital One never had any concerns regarding Amazon's commitment to security. *See* Ex. 1 (Fisk, Capital One 30(b)(6) Tr.) at 122:5–9.

D. Capital One Installed and Configured the Components of Its Card Production Account That the Hacker Exploited.

18. As an AWS customer, Capital One is responsible for the selection, configuration, and security of its operating systems, applications, or firewalls. Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 58:19–24; *see also* Ex. 26 (Schmidt Tr.) at 55:3–10 ("Security in the cloud is something that a customer is responsible for, and therefore, the customer has the decisions to make on how they are secured themselves.").

19. Capital One chooses and configures the applications, firewalls, and IAM permissions in its AWS accounts. *See* Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 23:4–6, 35:21–36:1, 57:2–20; Ex. 1 (Fisk, Capital One 30(b)(6) Tr.) at 101:1–2, 104:17–25, 106:2–13.

20. Capital One used [redacted] on an AWS virtual server. [redacted] Ex. 14 (Helou Ex. 230); Ex. 1 (Fisk, Capital One 30(b)(6) Tr.) at 47:7–48:6, 50:4–51:1.

21. Capital One installed the PONG application in one of its AWS accounts, named the Card Production account, also referred to as the Card Prod account. Ex. 8 (Lye, Capital One 30(b)(6) Tr.) at 22:11–25:19.

22. [redacted] Ex. 8 (Lye, Capital One 30(b)(6) Tr.) at 22:20–23:10. A WAF is a software tool that can be configured to limit access to

applications from the Internet. ModSec is an open source WAF. *Id.* at 22:11–25:19; Ex. 1 (Fisk, Capital One 30(b)(6) Tr.) at 99:2–102:2.

23. [redacted] Ex. 1 (Fisk, Capital One 30(b)(6) Tr.) at 101:1–102:2.

24. Although Amazon offers an AWS-developed WAF that customers can choose to use, Capital One did not use the AWS WAF [redacted] *See* Ex. 25 (Schuster, AWS 30(b)(6) Tr.) at 41:4–10 [redacted] *id.* at 77:20–23 ("Q. Are the Amazon-developed WAFs available to its customers as one of the services offered by Amazon? A. Yes, sir. It is.").

25. Amazon had no role in or knowledge of Capital One's use of [redacted] Ex. 1 (Fisk, Capital One 30(b)(6) Tr.) at 101:1–102:2; Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 29:19–22.

26. [redacted]

[redacted]

27. Amazon had no role in, or knowledge of, [redacted]

28. Capital One configured the Identity and Access Management permissions for [redacted] Ex. 1 (Fisk, Capital One 30(b)(6) Tr.) at 106:2–13; Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 30:2–8 (testifying that AWS did not set up IAM roles for Capital

One, because "IAM is one of the services that customers configure themselves that they own and operate as an AWS service"). Those permissions allowed the ModSec WAF role to list (identify) and get (download) data stored within certain S3 buckets associated with Capital One's Card Production account.

29. [redacted]

30. [redacted]

31. There is no evidence that Capital One's storage of Plaintiffs' account application data in [redacted] *See* Ex. 29 (Bentzen, AWS 30(b)(6) Tr.) at 51:19–52:23; Ex. 31 (Bentzen 30(b)(6) Ex. 773).

E. Investigation of the Cyber Incident.

32. Amazon incorporates by reference Capital One's Statement of Undisputed Material Facts (Dkt. 1462 at 2–11) ("Capital One SUMF") ¶¶ 1–8 regarding Capital One's July 29, 2019 announcement of the Cyber Incident and its two-week long investigation, including Capital One's remediation efforts following the investigation. Amazon further incorporates by reference Capital One SUMF ¶¶ 9–21, 26–48 regarding Plaintiffs' relationship with Capital One and their alleged damages, Plaintiffs' prior exposures of their PII, and prior misuses of Plaintiffs' PII.

33. [redacted] Ex. 21 (Capital One's Supplemental Responses to Interrogatories Nos. 10, 11, 13, and 14); Ex. 8 (Lye, Capital One 30(b)(6) Tr.) at 54:2–9.

34. On July 20, 2019, Capital One's Chief Information Security Officer ("CISO") [redacted]

35. Mr. Schmidt told Mr. Johnson that AWS would provide [redacted]

[redacted] *see* Ex. 25 (Schuster, AWS 30(b)(6) Tr.) at 29:20–30:5.

36. [redacted]

37. Capital One took responsibility for the Cyber Incident. *See* Ex. 6 (Caputo, Capital One 30(b)(6) Tr.) at 90:23–91:20 ("… Capital One is fully accountable for the cyber event that took place in July 2019.").

38. Following the July 2019 announcement of the Cyber Incident, Capital One continued its migration to AWS and completed that migration in October 2020. *See* Ex. 29 (Bentzen, AWS 30(b)(6) Tr.) at 100:9–18; Ex. 23 (Capital One's March 12, 2020 Amended Response to Interrogatory No. 20).

F. There Is No "Inherent Vulnerability" in AWS.

39. There is no SSRF vulnerability in the AWS metadata service. Ex. 27 (Schmidt, AWS 30(b)(6) Tr.) at 34:15–35:23 (stating the vulnerability that was exploited in this case is "a latent or present opportunity for an attacker to gain access because of a misdesign, misprogramming, [or] misconfiguration, of which there were none in the [AWS] metadata service").

40. Both Amazon and Capital One's investigations of the Cyber Incident concluded that there was no vulnerability on the AWS side of the shared responsibility model. Ex. 25 (Schuster, AWS 30(b)(6) Tr.) at 37:4–11 [redacted]

[redacted]

41. [redacted]

42. [redacted]

43. SSRF or Forgery attacks are not unique to intrusions in cloud environments and could equally take place on a web application running from an on-premise data center. *See* Ex. 48 (Madnick Tr.) at 34:19–35:2 (agreeing further that forgery attacks have occurred before the advent of cloud computing).

44. The forgery attack on Capital One's Card Production account could not have occurred without a customer misconfiguration. [redacted]

G. Amazon Did Not Develop or Market Cloud Custodian.

45. Cloud Custodian is a policy enforcement automation tool developed by Capital One to monitor the configuration of cloud environments and help its operations comply with their regulatory requirements. Ex. 1 (Fisk, Capital One 30(b)(6) Tr.) at 109:24–110:2; Ex. 10 (Walker, Capital One 30(b)(6) Tr.) at 77:8–78:14, 79:21–80:5; Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 158:20–159:2.

46. Cloud Custodian's function is to detect deviations from a set configuration and then take either reactive corrective action to change it or notify users that changes have occurred. Ex. 3 (Donovan, Capital One 30(b)(6) Tr.) at 19:20–20:12.

47. Cloud Custodian did not have the ability to detect the hacker's activity that led to the Cyber Incident. Ex. 1 (Fisk, Capital One 30(b)(6) Tr.) at 110:6–10. Cloud Custodian was not intended or designed to check for WAF configurations, IAM settings, or IAM rules within AWS. Ex. 10 (Walker, Capital One 30(b)(6) Tr.) at 85:9–86:11. Cloud Custodian does not monitor AWS's EC2 instances or the permissions that are granted to EC2 instances. Cloud Custodian does not detect or provide alerts of suspected intrusions into an AWS account. Ex. 3 (Donovan, Capital One 30(b)(6) Tr.) at 20:13–19.

48. Capital One developed Cloud Custodian and made its code available for free for others to use and modify as "open source" software. Ex. 10 (Walker, Capital One 30(b)(6) Tr.) at 77:8–14; Ex. 3 (Donovan, Capital One 30(b)(6) Tr.) at 21:10–12; Ex. 1 (Fisk, Capital One 30(b)(6) Tr.) at 109:21–110:2; Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 160:25–161:19.

49. AWS did not participate in Cloud Custodian's development. Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 156:12–20, 160:2–4 ("Q: Did Amazon have any role in the development of Cloud Custodian? A: We did not."); Ex. 10 (Walker, Capital One 30(b)(6) Tr.) at 83:18–20 ("Q: Was

AWS involved in the development of what would become Cloud Custodian? A: Not to my knowledge.").

H. Plaintiffs' Lack of Knowledge of AWS.

50. When Representative Plaintiff Emily Behar applied for a Capital One credit card in 2018, she was not aware that Capital One had a business relationship with Amazon, and that relationship therefore did not factor into her decision to apply for a Capital One account. Ex. 49 (Behar Tr.) at 178:21–25. Behar learned of AWS through her attorney a "couple months" before her July 17, 2020 deposition. *Id.* at 175:22–176:7. At the time of her deposition, Behar did not know anyone who used AWS as a service. *Id.* at 176:8–10. Nor had Behar ever visited AWS's website; seen any of AWS's commercials, advertisements, blog posts, press releases, or other public statements regarding security; or heard of Cloud Custodian. *Id.* at 176:8–20, 178:6–15.

51. [redacted]

52. Edmondson heard of AWS for the first time on the day of her deposition on November 13, 2020. Ex. 50 (Edmonson Tr.)at 204:2–4. Therefore, the existence of a relationship between Amazon and Capital One did not impact Edmondson's decision to apply for a Capital One credit card in 2008. *Id.* at 206:6–10. At the time of her deposition, Edmondson had never

seen any statements about the security of AWS's cloud services nor heard of Cloud Custodian. *Id.* at 205:2–7.

53. When Representative Plaintiff Brandon Hausauer applied for Capital One credit cards in 2011 and 2012, he was not aware that Capital One had a relationship with AWS. Ex. 53 (Hausauer Tr.) at 228:1–6. He first learned of that relationship after the Cyber Incident. *Id.* at 217:2–22, 222:15–223:3. Therefore, Capital One's relationship with AWS had no bearing on Hausauer's decision to open credit cards with Capital One. *Id.* at 228:1–6. Hausauer could not recall ever visiting AWS's website, nor having seen any specific AWS public statements, advertisements, press releases, or blog posts. *Id.* at 224:19–226:8. At the time of his deposition, Hausauer had not personally interacted with anybody who works for AWS nor personally engaged in business with AWS. *Id.* at 214:5–23. Hausauer testified that his knowledge of Cloud Custodian is "broad and superficial" and described it as "kind of an administrator-type application to help companies that are using AWS." *Id.* at 226:9–19.

54. When Representative Plaintiff Sara Sharp applied for Capital One cards [redacted] 2017, and 2018, she had not heard of AWS. Ex. 54 (Sharp Tr.) at 188:2–10. Sharp first learned of AWS's relationship with Capital One by reading the complaint "possibly three months, maybe four" before her June 25, 2020 deposition. *Id.* at 185:25–188:1. Thus, Capital One's relationship with AWS [redacted] *Id.* at 188:25–189:6. At the time of her deposition, Sharp had never visited AWS's webpage; seen any AWS advertisements or other public statements, or heard of Cloud Custodian outside of what she reviewed in the complaint. *Id.* at 186:14–21, 189:8–16.

55. At the time Representative Plaintiff Caralyn Tada last applied for a Capital One credit card [redacted] she had no knowledge of AWS. Ex. 56 (Tada Tr.) at 178:15–18. Tada testified

that she first learned of AWS when she [redacted] and she inaccurately described AWS as a service where "they were holding [her] pictures that [she] didn't have enough storage for on [her] phone." *Id.* at 176:4–25. At her deposition, Tada testified that she did not know anything about Capital One's relationship with AWS. *Id.* at 177:1416. Therefore, Capital One's relationship with AWS had no bearing on Tada's decision to apply for a Capital One credit card in 2015. *Id.* at 180:14–18. Tada had never visited AWS's website; seen any of AWS's advertisements, blog posts, press releases, or other public statements; or heard of Cloud Custodian. *Id.* at 177:1–10, 177:17–19.

56. Representative Plaintiff Emily Gershen applied for a Capital One card online in January 2015. *See* Ex. 52 (Gershen Tr.) at 66:12–23. Gershen first heard about AWS while watching the fictional television show Silicon Valley on HBO in May 2020. *See id.* at 228:6–21. She was not aware that Capital One had a business relationship with AWS prior to "reviewing documents filed in this case that stated AWS as a party." *Id.* at 230:8–20. At the time she applied for a Capital One credit card in early 2015, Gershen did not consider AWS in her decision to open a Capital One credit card. *Id.* at 233:21–234:8. At the time of her deposition, Gershen did not know anyone who utilized AWS's services as a customer. *Id.* at 229:5–7. Nor had Gershen ever visited AWS's website; seen any AWS advertisements, blogs, press releases, or any other public statements; or heard of Cloud Custodian. *Id.* at 229:8–23, 231:10–18.

57. Representative Plaintiff John Spacek testified that at the time he applied for a Capital One credit card [redacted] he could not recall being aware of Capital One's business relationship with Amazon. Ex. 55 (Spacek Tr.) at 240:22–24, 242:24–244:11. Spacek testified that he "think[s] [he has] probably heard of [AWS] prior to this [incident] in some form or fashion" and that he had "maybe seen them, you know, through financial stuff," but was unable to recall

specifically when or how he had first heard of AWS. *Id.* at 238:5–239:9, 242:14–23. Spacek testified that Capital One's relationship with AWS did not influence his decision to apply for a Capital One credit card. *Id.* at 247:11–23. At the time of his deposition, Spacek did not know anyone who used AWS's services as a customer. *Id.* at 239:17–19. Nor had Spacek ever visited AWS's website; see any of AWS's blog posts, press releases, or other published statements; or hear of Cloud Custodian. *Id.* at 240:4–16, 242:1–3.

58. At the time that Representative Plaintiff Gary Zielicke opened his Capital One credit card account in July of 2018, he had not heard of AWS. Ex. 57 (Zielicke Tr.) at 176:12–15. Zielicke testified that he had not heard of AWS and "really d[id]n't know anything about them." *Id.* at 173:13–22. He was not aware that Capital One had a business relationship with Amazon until "a couple of days" before his deposition. *Id.* at 174:25–175:10, 176:16–19. At the time of his deposition, Zielicke did not know anyone who was a customer of AWS. *Id.* at 174:14–16. Nor had Zielicke ever visited AWS's website; seen any of AWS's advertisements, press releases, or blog posts; or heard of Cloud Custodian. *Id.* at 174:17–24, 176:1–3.

LEGAL STANDARD

The Court "shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). A party moving for summary judgment "discharges its burden by showing that there is an absence of evidence to support the nonmoving party's case." *Humphreys & Partners Architects, L.P. v. Lessard Design, Inc.*, 790 F.3d 532, 540 (4th Cir. 2015). Rule 56 "mandates the entry of summary judgment … against a party who fails to make a showing sufficient to

establish the existence of an element essential to that party's case … on which that party will bear the burden of proof at trial." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986).

ARGUMENT

I. AMAZON IS ENTITLED TO SUMMARY JUDGMENT ON PLAINTIFFS' NEGLIGENCE CLAIM (COUNT 1).

To establish a cause of action for negligence, Plaintiffs must prove: (1) the existence of a legal duty; (2) breach of that duty; (3) proximate causation; and (4) compensable damages. *See Goddard v. Protective Life Corp.,* 82 F. Supp. 2d 545, 551 (E.D. Va. 2000) (citations omitted); *Atrium Unit Owners Ass'n v. King*, 585 S.E.2d 545, 548 (Va. 2003) (stating elements of negligence claim). Plaintiffs' negligence claim against Amazon fails because: (1) Plaintiffs do not—and cannot—establish that Amazon owed Plaintiffs a duty of care to protect Plaintiffs' PII that Amazon did not acquire or maintain, and which was under Capital One's control;[3] and (2) Plaintiffs cannot establish that Amazon was the proximate cause of any harm to Plaintiffs.[4]

A. Amazon Does Not Owe a Duty of Care to Plaintiffs.

According to Plaintiffs, Amazon owed them a duty to protect their PII from the Cyber Incident based on AWS's alleged affirmative acts and representations regarding AWS security. *See* Compl. ¶¶ 50-59, 60-75, 100-108. But a year of discovery has shown that the *allegations* in the Complaint that the Court relied on to conclude that Plaintiffs had adequately *pled* a duty of

---

[3] The Court dismissed Plaintiffs' negligence *per se* claim (Count 2) to the extent the claim was governed by Virginia law. Order at 37. To the extent any non-Virginia Plaintiffs had negligence *per se* claims following the Motion to Dismiss Order, the Court's order holding that Virginia law applies (Dkt. 1293) extinguishes those claims.

[4] Capital One's Motion for Summary Judgement (Dkt. 1463, Argument Sections I.A, 1–4) summarizes the lack of harm and compensable damages alleged by Plaintiffs. Amazon adopts that discussion and incorporates it here.

care as to Amazon are unsupported by the facts. *See* Order Granting in Part Defs.' Mots. to Dismiss, Dkt. 879 ("Order") at 21–24 (citing Compl. ¶¶ 26-34, 44-75, 96-98, 100-108, 161).

Where there is no legal duty to exercise care, there is no actionable negligence. *Veale v. Norfolk & W. Ry. Co.*, 139 S.E.2d 797, 799 (Va. 1965). Under Virginia law, a person generally has no duty to protect another from the criminal acts of a third-party absent a special relationship. *Burdette v. Marks*, 421 S.E.2d 419, 420–21 (Va. 1992); *Fox v. Custis*, 372 S.E.2d 373, 375 (Va. 1988) (citations omitted) (affirming the judgment of the trial court dismissing the action because no special relationship had been created that would support the finding of a duty); *see also* Restatement of Torts (Second) § 315 (1965). While a duty can be independently assumed where the defendant either "explicitly or implicitly" "engage[d] in some affirmative act amounting to rendering of services to another," the undisputed material facts in this case show no such conduct by Amazon. *See Bosworth v. Vornado Realty L.P.*, 83 Va. Cir. 549, 557 (2010) (citing *Fruiterman v. Granata*, 668 S.E.2d 127, 137 (Va. 2008)); *see also Terry v. Irish Fleet, Inc.*, 818 S.E.2d 788, 793 (Va. 2018).

As established below, (1) Plaintiffs have failed to identify a standard of care applicable to a cloud computing services provider, (2) there is no conduct by Amazon from which an assumption of a duty could be imputed, (3) there is no actual or special relationship between Plaintiffs and Amazon, and (4) the economic loss doctrine bars Plaintiffs' claims.

1. Plaintiffs Do Not Identify an Applicable Standard of Care.

The burden is on Plaintiffs to establish the elements of their claim, and there are no facts by which they can establish a standard of care applicable to Amazon as a provider of cloud computing services. Plaintiffs rely on their expert, Stuart Madnick, to support their allegation that Amazon acted negligently. But Professor Madnick did not identify a standard of care for providers of cloud computing services like AWS. An expert cannot opine that a defendant failed to meet a

standard of care without first defining that standard. *See Silverpop Sys., Inc. v. Leading Mkt. Techs., Inc.*, 641 F. App'x 849, 852 (2016) (per curiam) (affirming summary judgment for defendant in data breach case where plaintiff failed to identify a standard of care in the industry). The standard must be an objective measure that has been independently developed, tested, and challenged. *Dunn v. Ronbotics Corp.,* No. CIV.A. 02-952-A, 2002 WL 32591881, at *2 (E.D. Va. Dec. 12, 2002) (excluding expert's report since it used no methodology or recognized principles, no technique that could be tested, had not been subject to peer review, and contained no citations to any objective authority).

As explained in greater detail in both Capital One and Amazon's *Daubert* motions to exclude Madnick's opinions, Plaintiffs have not identified a standard of care based on any articulable or tested methodology, whether an industry standard or Madnick's own experience. While Madnick gives lip service to the NIST cybersecurity framework in his opinions as to Capital One, he is noticeably silent on evaluating AWS against any standard other than his *ipse dixet* statements that [redacted] And the only personal experience with cloud computing Madnick could identify were early IBM systems confined to the MIT campus nearly a half-century ago. Because they cannot identify a standard of care, Plaintiffs' negligence claims must be dismissed.

2. Amazon Did Not Voluntarily Assume a Duty of Care to Plaintiffs.

This Court previously held that the Complaint's allegation that Amazon assumed a duty of care to protect Plaintiffs' PII from theft was sufficient to plead a claim for negligence. *See* Order at 18–24. But after extensive discovery, the undisputed facts show that: (1) the Cyber Incident was not foreseeable to AWS; and (2) AWS did not make any representations to Plaintiffs about the security of their personal information.

a. The Cyber Incident Was Not Foreseeable to Amazon.

The Cyber Incident was not foreseeable to Amazon because the facts are undisputed that Capital One alone was responsible for the [redacted] and Amazon had no knowledge or control over those configurations. The record is undisputed that a criminal hacker was able to gain unauthorized access to Plaintiffs' PII [redacted] Absent that unique combination of configurations, the Cyber Incident could not have occurred.

The facts are undisputed that AWS had no role in or knowledge of any of those configurations. SUMF ¶¶ 21, 25, 27, 29–30. [redacted] Ex. 24 (Haken, AWS 30(b)(6) Tr.) at 58:19–24; *see* SUMF ¶¶ 8, 10, 18–19. [redacted] *See*

SUMF ¶¶ 7–11, 18. [redacted] *See* SUMF ¶ 10; *see also* Ex. 25 (Schuster, AWS 30(b)(6) Tr.) at 116:2–20 [redacted]

Absent knowledge of the customer-controlled configurations that the hacker exploited, and the types of data that [redacted] the Cyber Incident plainly was not foreseeable to AWS.

Plaintiffs' allegation that the Cyber Incident was foreseeable because AWS had an "inherent vulnerability" to SSRF or other forms of forgery attacks is unsupported by the undisputed facts. *See* Compl. ¶¶ 44, 50–59, 68. The record is clear that there is no such vulnerability in the AWS instance metadata service or infrastructure. [redacted] Ex. 27 (Schmidt, AWS 30(b)(6) Tr.) at 34:9–36:3); SUMF 38. The only vulnerability to SSRF attacks is one created [redacted] SUMF ¶ 43. [redacted]

[redacted]

Finally, the facts refute Plaintiffs' allegation that Amazon and Capital One's alleged "joint development" of Cloud Custodian show the foreseeability of the Cyber Incident. Compl. ¶¶ 44-59,

161). First, the record is clear that Amazon had no role in developing or maintaining Cloud Custodian. SUMF ¶ 45, 48–49. Rather, Capital One alone developed the open source code for Cloud Custodian for anyone to utilize. SUMF ¶ 48–49. Both Amazon and Capital One witnesses testified that AWS played *no* role in Cloud Custodian's development. SUMF ¶ 48–49. It is also undisputed that Cloud Custodian is not a security tool designed to protect personal data from third party exfiltration or even detect intrusions, but is an administrative tool developed by Capital One to help it manage its different cloud accounts and services. SUMF ¶¶ 45–47. Tellingly, Plaintiffs' technical expert, Madnick, does not even mention Cloud Custodian in his report.

There is no evidence whatsoever that the Cyber Incident was foreseeable to AWS to support a finding that AWS adopted a duty to protect Plaintiffs' PII from the incident.

b. Amazon Did Not Assume a Duty of Care to Plaintiffs Through Acts or Representations.

Plaintiffs allege that they each entrusted their sensitive PII to "Defendants" with the understanding that it would be kept safe based on "Defendants'" "statements and representations." Compl. ¶¶ 16, 40–45. But no Plaintiff identified a single AWS "statement" or "representation" to any Plaintiff about the security of their PII. The evidence shows that AWS never undertook or participated in any affirmative act or representation upon which a finding of a voluntary assumption of duty can be predicated.

No Representative Plaintiff was aware of Capital One's business relationship with AWS prior to the Cyber Incident. SUMF ¶¶ 50, 52–58. In fact, most had never heard of AWS until their lawyers filed lawsuits in the MDL proceedings beginning in August 2019, or, in some instances, only several days before their depositions. *Id.* ¶¶ 50, 52, 54, 56, 58. Plaintiff Zielicke learned of AWS for the first time on the day of his deposition. *Id.* ¶ 58.

Even those few Representative Plaintiffs who had some limited awareness of AWS did not know that Capital One stored its customers' personal data with AWS prior to this litigation. SUMF ¶¶ 53, 55, 57. Most of the Representative Plaintiffs had never visited the AWS website, seen a press release by AWS, seen a blog post by AWS, or seen any statement by AWS. SUMF ¶¶ 50, 52–58. And none could recall seeing a statement regarding the software tool Cloud Custodian, as further explained below. *Id.* Most pertinently, Capital One's storage of Plaintiffs' data with AWS was not a factor in any Representative Plaintiff's decision to apply for or continue using a Capital One credit card. *Id.*[5] In sum, it is undisputed that no Representative Plaintiff had seen, let alone could have considered or relied upon, any statements by AWS about its security or its cloud computing services to Capital One before they applied for and used their Capital One accounts.

In its order denying Defendants' motions to dismiss, the Court pointed to the Complaint's allegations that Defendants' statements about Cloud Custodian—which, as noted above, was open source software developed by Capital One was sufficient to plead that AWSa duty to Plaintiffs. But discovery revealed that no Representative Plaintiff could recall any statement about Cloud Custodian, and seven never even heard of it. SUMF ¶¶ 50, 52–58. The only Representative Plaintiff who testified that he had heard of Cloud Custodian admitted his knowledge was "really just broad and superficial," and described the "Cloud Custodian card" as a "kind of an administrator-type application to help companies that are using AWS." SUMF ¶ 53. Those admissions forecloses any argument that AWS assumed a duty to Plaintiffs by reason of alleged representations regarding Cloud Custodian. SUMF ¶¶ 50, 52–58.

---

[5] And as stated in Amazon's Opposition to Plaintiffs' Motion for Class Certification (Dkt. No. 1435) at 5, members of the putative class who applied for Capital One credit cards before their data was migrated to AWS between 2015 and 2020 logically cannot show any theory of reliance against Amazon.

In sum, the undisputed material acts show that Amazon did not voluntarily undertake a duty to protect Plaintiffs' PII from the Cyber Incident.

3. Amazon Owes No Common Law Duty of Care to Plaintiffs.

a. There Is No Common Law Duty in Virginia to Protect Individuals' PII from an Electronic Data Breach.

Because the undisputed facts do not support a finding that Amazon assumed a duty to protect Plaintiffs' PII from theft by a criminal hacker, the only possible remaining basis for the finding of a duty of care is a common law duty. But because Virginia does not recognize a common law duty to protect personal data from theft by third parties, Amazon is entitled to summary judgment. *See Deutsche Bank Nat'l Tr. Co. v. Buck*, No. 3:17CV833, 2019 WL 1440280, at *6 (E.D. Va. Mar. 29, 2019); *Parker v. Carilion Clinic*, 819 S.E.2d 809 (Va. 2018). "In only rare circumstances has [the Supreme Court of Virginia] determined that [a] duty to protect against harm from third party criminal acts exists." *Commonwealth v. Peterson*, 749 S.E.2d 307, 312 (Va. 2013); *Yuzefovsky v. St. John's Wood Apartments*, 540 S.E.2d 134, 139 (Va. 2001) (same).

Parker and *Buck* are dispositive here. While the Complaint alleges that Capital One solicited customers' PII and aggregated and "mine[d]" data to "boost its profits" (Compl. ¶¶ 26-34), the facts are undisputed that AWS *did not* solicit or use any information from Plaintiffs. No representative Plaintiff could identify any statements by AWS relating to Capital One, and all of them admitted that Capital One's use of AWS in this regard had no bearing on their decisions to apply for or use Capital One accounts. SUMF ¶¶ 50–58. The facts are also undisputed that AWS did not use any of Plaintiffs' PII, aggregate it, or mine that data to "boost its profits." SUMF ¶ 5. In fact, AWS's Contracts with Capital One prohibit AWS from using or accessing Capital One's customers' data for any purpose. SUMF ¶ 4.

Accordingly, there is no basis to find that Amazon owed a common law duty to Plaintiffs.

b. There Is No Actual or Special Relationship Between Amazon and Plaintiffs.

Plaintiffs allege that Amazon's duty to secure Plaintiffs' PII arose as a result of the "special relationship" between AWS and Plaintiffs and class members. Compl. ¶ 163. Virginia law recognizes an assumed duty to pprotect another from third-party criminal conduct only when: (i) the parties have a "special relationship" akin to business owner/invitee and the defendant has reason to know of a specific, immediate threat to the plaintiff, or (ii) when the defendant "expressly communicates" its specific undertaking to plaintiff. *See Terry*, 818 S.E.2d at 792. Discovery has shown that no such relationship exists.

There is no special relationship between AWS and Plaintiffs from which an assumed duty of care could be found. Traditional examples of relationships that satisfy the narrow "special relationship" exception are common carrier-passenger, business proprietor-invitee, innkeeper-guest, and employer-employee. *See Kellermann v. McDonough*, 684 S.E.2d 786, 793 (Va. 2009). Absent such a relationship, AWS owes no duty of care to Plaintiffs. *Eisenberg v. Wachovia Bank, N.A.*, 301 F.3d 220, 226–27 (4th Cir. 2002) (holding that a bank owed no duty of care to a noncustomer who was defrauded by a bank depositor, since the bank did not have a direct relationship with the noncustomer). None of these relationships applies or is analogous here.

It is undisputed that Plaintiffs' sole relationship was with Capital One and not AWS. The evidence not only confirms the absence of a relationship between AWS and Plaintiffs but makes clear that Plaintiffs did not even know of AWS or consider it in any way when applying for and using their Capital One cards. SUMF ¶¶ 50–58. In fact, five out of the eight Representative Plaintiffs had never heard of AWS *at all* prior to this litigation. SUMF ⁋⁋ 50, 52, 53, 56, 58. Those that had heard of AWS had only a general, and sometimes inaccurate, awareness of what AWS

does. SUMF ¶¶ 53, 55, 57. Absent a special relationship, there can be no finding that AWS owed a duty of care to Plaintiffs.

4. The Economic Loss Doctrine Bars Plaintiffs' Claims.

Under Virginia law, the economic loss doctrine bars Plaintiffs' claims as to Amazon for two independent reasons.

First, because Plaintiffs cannot show that AWS voluntarily assumed a duty, the "source of duty" rule is inapplicable as to AWS. The source of duty rule permits a party to assert a tort claim if the underlying duty arises independent of any contractual duties or convents. *See* Order at 20. In other words, "where a contract exists between parties and one party brings an action in tort, that plaintiff must allege a common law duty for the protection of persons or property that exists in tort law, independent of any duty owed solely by virtue of the contract." *All Am. Ins. Co. v. James River Petroleum, Inc.*, No. 3:21CV8, 2021 WL 2284608, at *2 (E.D. Va. June 4, 2021) (finding the source of duty rule barred Plaintiffs' negligence claims because defendant did not have a common law duty to prevent a third party criminal act). As explained above, Plaintiffs cannot establish any common law duty that Amazon owed them. Thus, the source of duty rule is inapplicable as to Amazon.

Second, Plaintiffs' negligence claim must fail because, as shown by the report of Gary Olsen, Plaintiffs' damages expert, they seek only economic losses. *See* Dkt. 1430-01, Exhibit A. Virginia law does not allow tort damages for economic losses absent a physical impact to person or property. *See Blake Constr. Co. v. Alley*, 353 S.E.2d 724, 726 (Va. 1987) (finding "[t]here can be no actionable negligence where there is no breach of a duty 'to take care for the safety of the person or property of another.'"); *Sensenbrenner v. Rust, Orling & Neale, Architects, Inc.,* 374 S.E.2d 55, 58 (Va. 1988) (finding that Virginia law does not permit recovery by a plaintiff against third parties where the plaintiff alleges nothing more than disappointed economic expectations and

the parties are not in privity of contract). Discovery has shown that Plaintiffs not only did not suffer any economic losses, they also did not suffer any personal or property injuries. Capital One's Motion for Summary Judgment describes in detail Plaintiffs' purely economic alleged losses and also explains why Plaintiffs may not recover for "lost time," inconvenience, or other non-economic harms under Virginia law. *See* Dkt. 1463 at 19. Amazon adopts and incorporates those same arguments as to the negligence claims against Amazon.

B. Plaintiffs Cannot Establish That Amazon Proximately Caused Any Alleged Injuries.

Plaintiffs also cannot sustain a claim for negligence because there is no evidence from which a jury could reasonably conclude that Plaintiffs suffered any injury proximately caused by Amazon. "The proximate cause of an event is that act or omission which, in natural and continuous sequence, unbroken by an efficient intervening cause, produces the event, and without which that event would not have occurred." *Atrium Unit Owners Ass'n*, 585 S.E.2d at 548; *see also Interim Personnel of Cent. Va., Inc. v. Messer*, 559 S.E.2d 704, 708 (Va. 2002). Negligence always requires a showing of proximate causation and can never be presumed from the mere occurrence of injury. *Town of W. Point v. Evans*, 224 S.E.2d 349, 350–351 (Va. 1983). Under Virginia law, "something *more* is required than 'simplistic but for causation' to resolve the proximate cause question." *Benedict v. Hankook Tire Co.,* 286 F. Supp. 3d 785, 790 (E.D. Va. 2018) (citing *Banks v. City of Richmond*, 348 S.E.2d 280, 283 (Va. 1986) (emphasis added)). Plaintiffs allege that "as a direct and proximate result" of Amazon's negligence, Plaintiffs and class members have been "injured." Compl. ¶ 169. But after extensive fact and expert discovery, the undisputed facts are

that Amazon did not cause, control, or know about Capital One's configurations that the hacker exploited.[6] SUMF ¶¶ 18–19, 25, 27, 29.

1. The Breach Was Caused by a Criminal Hacker's Exploitation of Configurations of Capital One's Card Production Account that Amazon Did Not Know About, Cause, or Control.

The Cyber Incident was not proximately caused by any conduct or inaction by Amazon. [redacted] SUMF ¶¶ 18–30. Capital One, like all of AWS's other millions of customers, chooses and configures its own firewalls and IAM permissions. SUMF ¶¶ 18–19. [redacted] SUMF ¶¶ 19, 22, 26, 28. And, as discussed above, [redacted] SUMF ¶¶ 39–42.

[redacted] *See* SUMF ¶¶ 37, 40–41. Amazon reached the same conclusion. SUMF ¶¶ 39–40. Even Plaintiffs' own expert, Madnick, admitted that, [redacted] SUMF ¶ 4.

Accordingly, the facts are undisputed that Amazon did not proximately cause the Cyber Incident.

[6] Capital One's Motion for Summary Judgment explains that a mere increased risk of suffering harm in the future is not a legally cognizable injury under Virginia tort law. Dkt. 1463 at 15–19. Amazon adopts that discussion and incorporates it here.

2. Any Causal Link to the Injuries Plaintiffs Claim Is Pure Speculation.

Finally, although Plaintiffs claim they suffered identity theft and fraud, Plaintiffs do not establish through the evidence that those harms were *caused* by the Cyber Incident. Plaintiffs cannot prove a causal link to their alleged injuries because there is no evidence whatsoever that the hacker, who was arrested, disseminated any of the data that she acquired in the Cyber Incident before she was apprehended and law enforcement recovered the stolen data. Merely alleging that fraud or identity theft occurred at some point after the Cyber Incident does not plead causation at all, because it fails to establish that the required causal nexus "is a *probability* rather than a *mere possibility*." *Atrium Unit Owners Ass'n*, 585 S.E.2d at 548 (emphasis added); *see also Wilkins v. Sibley*, 135 S.E.2d 765, 767 (Va. 1964) (mere "'possibility' of causal connection is not sufficient" to establish proximate causation).

Capital One's Motion for Summary Judgment covers in detail why no reasonable jury could find that Plaintiffs suffered legally cognizable injuries or damages proximately caused by the Cyber Incident, because there is no evidence that any alleged fraudulent activity was committed using information obtained in the Cyber Incident. Dkt. 1463 at 13–17. Amazon adopts that discussion and incorporates it here.

II. AMAZON IS ENTITLED TO SUMMARY JUDGMENT ON PLAINTIFFS' UNJUST ENRICHMENT CLAIM (COUNT 3).

To prevail on their unjust enrichment claim under Virginia law, Plaintiffs must prove that (1) they conferred a benefit on Amazon, (2) Amazon knew of the benefit and should reasonably have expected to repay Plaintiffs, and (3) Amazon accepted or retained the benefits provided by Plaintiffs without paying for its value. *T. Musgrove Constr. Co. v. Young*, 840 S.E.2d 337, 341 (Va. 2020); *Schmidt v. Household Fin. Corp., II*, 661 S.E.2d 834, 838 (Va. 2008). As an initial matter, for the reasons stated in Section II.C. of Amazon's opposition to Plaintiffs' motion for

class certification, Plaintiffs lack Article III standing to assert an unjust enrichment claim because they cannot prove that Amazon was unjustly enriched at their expense. *See* Dkt. 35 at 12-16. Additionally, Amazon is entitled to summary judgment on this claim for three reasons. First, Plaintiffs have adduced no evidence that they conferred a benefit on AWS. Plaintiffs provided their PII to Capital One, not AWS, in return for credit card services, and AWS made no use of the data that Capital One elected to store in its AWS accounts. Second, there is no evidence [redacted] nor is there any factual basis to support a finding that AWS should reasonably have expected to pay Plaintiffs for Capital One's storage of their data in Capital One's AWS accounts. Third, [redacted] *See* SUMF ¶ 31, Dkt. 1430-01, Exhibit A ¶¶ 10, 64, 65.

A. Plaintiffs Did Not Confer a Benefit on Amazon.

To succeed on a claim for unjust enrichment, plaintiffs must first establish that he or she conferred a benefit upon defendants. *See Devil's Advoc., LLC v. Zurich Am. Ins. Co.,* 666 F. App'x 256, 261 (4th Cir. 2016) (per curiam). Absent some interaction between AWS and Plaintiffs with respect to their PII, they cannot prevail on their unjust enrichment claim. *See Seeman v. Oxfordshire, LLC*, 83 Va. Cir. 442 (2011) (dismissing a homeowner's unjust enrichment claim against drywall manufacturers where there was no allegation that plaintiff and defendant "ever dealt directly with each other"). The facts are undisputed that Plaintiffs did not provide their PII to AWS, they had no interactions with AWS, and AWS did not benefit or profit from the PII that Plaintiffs provided to Capital One.

Plaintiffs allege that they conferred their PII on "Defendants," but there is no evidence that they conveyed their PII to AWS. Plaintiffs provided their data to Capital One to apply for credit

card services. Several of the Representative Plaintiffs applied years before Capital One even began migrating its information technology to the cloud, and some applied in paper form. SUMF ¶¶ 51, 53. Separately, Capital One paid AWS in exchange for cloud storage and computing services. *See* SUMF ¶¶ 1, 3. There is no evidence that Plaintiffs conferred their data to AWS, because they did not. The facts are further undisputed that AWS did not access or use Plaintiffs' data to its benefit or otherwise. In fact, [redacted] SUMF ¶ 4–5.

Plaintiffs readily acknowledged that they did not provide their personal information to AWS. Not a single Representative Plaintiff had any knowledge of AWS's business relationship with Capital One before the underlying lawsuits were filed in August 2019. *See* SUMF ¶¶ 50, 52–58. Only three Representative Plaintiffs had any awareness of AWS before this lawsuit: Brandon Hausauer, John Spacek, and Caralyn Tada. But their knowledge was superficial, at best. SUMF ¶¶ 53, 55, 57. Such awareness would have been impossible for Edmonson, Gershen, Hausauer, and Tada who applied for Capital One accounts before Capital One migrated its technology infrastructure to AWS. And each Representative Plaintiff expressly acknowledged that Capital One's storage of data in AWS accounts was *not* a factor in their decision to apply for or continue using their Capital One accounts. *See* SUMF ¶¶ 50–58.

As a matter of law, Plaintiffs cannot show that they conferred a benefit on Amazon when the facts are undisputed that Capital One independently chose to store Plaintiffs' PII in its AWS accounts for Capital One's use, and AWS made no use of the PII.

B. There Is No Evidence that Amazon Should Have Reasonably Expected to Pay Plaintiffs for Data that Capital One Stored in Its AWS Accounts.

There are no facts to support a finding that AWS should have reasonably expected to pay Plaintiffs for their PII, because the facts are undisputed that AWS did not know about or have

access to the data Capital One stored in its AWS accounts, and AWS made no use of Plaintiffs' PII. Under Virginia law, a plaintiff cannot prevail on an unjust enrichment claim under Virginia law where there is no evidence that the defendant knew of the benefit allegedly conveyed to it by the Plaintiff or that the defendant used and enjoyed that benefit. *See Firestone v. Wiley*, 485 F. Supp. 2d 694, 704 n.12 (E.D. Va. 2007) (quoting *Eckstone & Assoc. Ltd. v. Keilp,* 1995 Va. Cir. LEXIS 1404, at *3–4 (Va. Cir. 1995) (dismissing unjust enrichment claim where plaintiff failed to allege the defendant knew of an appraisal report she commissioned or that the defendant used that report)). There is no evidence that AWS had any visibility into the types of data, let alone the individuals associated with that data, stored by AWS customers in their AWS accounts. Furthermore, there is no evidence that AWS ever pays the individuals associated with data that AWS's customers store in their AWS accounts. Because AWS did not know of any benefit conferred by the Plaintiffs, AWS obviously could not have had a reasonable expectation to repay them. *T. Musgrove*, 840 S.E.2d at 341.

Additionally, because AWS provides services to its customers who contract with AWS, its only reasonable expectation is that it would provide cloud computing services to Capital One in return for Capital One's payments. [redacted] *See* SUMF ¶¶ 1–4. There is no evidence in this case that AWS knew it was receiving Plaintiffs' PII contained in credit card account applications or that AWS made any use of that PII. The evidence is to the contrary; Amazon made *no use whatsoever* of Plaintiffs' PII. SUMF ¶¶ 4–5. [redacted] *See* SUMF ¶ 4. Indeed, until this litigation, [redacted]

[redacted] SUMF ¶ 30. The evidence also refutes Plaintiffs' allegations that AWS uses, processes, or monetizes Plaintiffs' data. SUMF ¶ 5. Accordingly, AWS did not know of any "benefit" Plaintiffs conferred on AWS and certainly had no reasonable expectation to repay Plaintiffs for the PII they shared with Capital One.

Courts applying Virginia law have found that a Plaintiff cannot show that a defendant accepted or retained the benefit conferred by the plaintiff with an expectation of paying for its value where the defendant provided products or services to a third party that in turn had the direct relationship with the plaintiff. *See Staltzer v. Am. Merchant, Inc.*, No. 1:19CV00023, 2020 WL 7023892, at *4 (W.D. Va. Nov. 30, 2020); *Burch v. Whirlpool Corp.*, No. 1:17-CV-18, 2017 WL 7370988, at *7 (W.D. Mich. Sept. 28, 2017). In *Staltzer,* the plaintiff alleged that he provided government-grant consulting services to a subcontractor for a site-location contractor by the defendant to identify a site for a manufacturing plant. The defendant obtained grants to offset the cost of building the plant and the plaintiff claimed that he was never paid for his grant-consulting services. Rejecting the plaintiff's claim for unjust enrichment, the court held that the defendant could not have reasonably expected to pay the plaintiff, because the defendant only contracted with and expected to pay the site-location contractor. Likewise here, AWS's contract with Capital One shows that AWS's only reasonable expectation was that it would provide cloud computing services to Capital One and be paid for those services.

In *Burch*, a purchaser of a Whirlpool dishwasher with an allegedly defective part sought unjust enrichment damages from Whirlpool for replacement parts he bought from a third-party reseller. The court rejected the plaintiff's theory that Whirlpool accepted a benefit without payment when the plaintiffs purchased replacement parts through resellers, because Whirlpool

provided value by supplying the replacement parts to the resellers. Similarly, here, the facts are undisputed that Amazon provided value by providing cloud computing services to Capital One, which, in turn, provided banking and credit services to Plaintiffs. *See also Sky Cable, LLC v. Coley*, No. 5:11CV00048, 2013 WL 3517337, at *15 (W.D. Va. July 11, 2013) (granting summary judgment for unjust enrichment claim brought by regional distributor of satellite TV service against resort for underpayment of fees where claims were "entirely derivative" of the resort's contract with the satellite service provider).

Courts applying Virginia law have also dismissed unjust enrichment claims where there was no history of the defendant paying the plaintiff in similar circumstances. In *Rosetta Stone Ltd. v. Google, Inc*., for example, Rosetta Stone alleged that Google unjustly enriched itself by using Rosetta Stone trademarks as keywords for Internet search advertisements for competitors. 676 F.3d 144, 166 (4th Cir. 2012). The Fourth Circuit affirmed dismissal because there was no allegation that Google had ever paid brand owners for these types of ad campaigns. Therefore, there was no basis that Google would reasonably expect to pay Rosetta Stone. *Id.* Similarly here, there are no facts showing that AWS reasonably expects that it will provide payment to its business customers' end users or customers with whom it has no relationship or interactions.

Because there are no facts that AWS reasonably would have been expected to pay Plaintiffs for their PII they provided to Capital One and that Capital One stored in its AWS accounts, summary judgment should be granted to Amazon on Plaintiffs' unjust enrichment claim.

C. No Facts Support Plaintiffs' Theory that the Entirety of Amazon's Profits from Providing Cloud Computing Services to Capital One Is a Proper Measure of Unjust Enrichment.

Plaintiffs' overreaching claim that Amazon should disgorge *all* profits from *all* services provided to Capital One from 2015 through 2020 has no basis in the facts, nor in principles of law and equity. There are no documents, testimony, or other data supporting Plaintiffs' claim that the

entirety of profits earned by AWS for providing cloud computing services to Capital One over more than five years are attributable or traceable to Capital One's storage of the impacted applicant and cardholder information in the Card Production account. When a company's profits would have been the same with or without the plaintiff, then the company did not unjustly benefit or gain *from the plaintiff*. *Mullins v. Equitable Prod. Co.*, No. 2:03-CV-00001, 2003 WL 21754819, at *4–5 (W.D. Va. July 29, 2003) (rejecting an unjust enrichment profits award where profits would have been the same had the gas company passed through any other land). Here, there is no evidence that Capital One's storage of the impacted applicant and cardholder information in its AWS accounts had any measurable impact on AWS's profits from providing cloud computing services to Capital One.

Plaintiffs' only basis for this theory is the unreliable testimony of their expert Gary Olsen, who opines that [redacted] SUMF ¶ 31. As explained in Amazon's *Daubert* motion to exclude Olsen's testimony, his opinion is unreliable and should be excluded in its entirety. *See* Dkt. 1430 (Amazon's Motion to Exclude Testimony of Gary Olsen). Olsen based his unjust enrichment theory on the speculative premise that [redacted] SUMF ¶ 31. But Olsen's speculation is directly contradicted by the undisputed facts. [redacted] SUMF ¶ 38. Furthermore, Capital One's corporate representative testified that [redacted] SUMF ¶ 17.

There is no evidence that Capital One's storage of [redacted]

[redacted] SUMF ¶ 31. There is no dispute that [redacted] SUMF ¶¶ 3–4. [redacted] The hacker exfiltrated [redacted] SUMF ¶ 33. The benefits AWS received from Capital One were payments for the full suite of AWS services, not any benefit from Plaintiffs' PII.

The unjust enrichment remedy sought by Plaintiffs also violates the core principles of equity in which unjust enrichment is rooted. No court has applied an unjust enrichment remedy in a data breach case, let alone a data breach case against a service provider that had no relationship with the consumer plaintiffs. But by analogy, in intellectual property infringement cases, courts have held that the disgorgement of profits must be limited to the portion of the profits attributable to the infringement. *See, e.g., Walker v. Forbes, Inc.*, 28 F.3d 409, 412 (4th Cir. 1994) (limiting disgorgement remedy in copyright infringement action brought against magazine to only those profits which were attributable to the infringing content—the photograph taken by the plaintiff—rather than profits from the sale of the magazine containing the photograph). Similarly, in real property trespass cases, courts limit disgorgement to the profits attributable to the trespass. *See, e.g.*, *Lodal v. Verizon Va., Inc.*, 74 Va. Cir. 110, 110–11, 116 (Cir. Ct. 2007) (limiting landowner's disgorgement remedy to the scope of a utility company's trespass in laying fiber cable across the property, rather than the utility company's entire profits). Here, however, there is no evidence supporting Plaintiffs' theory that AWS benefited at all from Plaintiffs' PII, let alone that the

entirety of the profits AWS has earned from providing cloud computing services to Capital One are somehow a result of or traceable to that PII.

III. AMAZON IS ENTITLED TO SUMMARY JUDGMENT ON PLAINTIFFS' STATE LAW STATUTORY CLAIMS.

A. California UCL and CLRA Claims (Counts 8 and 9): Plaintiffs Suffered No Injury Caused by Deceptive Conduct by Amazon.

To prove a violation of California's Unfair Competition Law (UCL), Plaintiffs must demonstrate that they "suffered an injury in fact" and lost money or property as a result of a defendant's alleged unfair, deceptive, or fraudulent business practice. Cal. Bus. & Prof. Code § 17204. Inherent in the requirement that a plaintiff have "suffered injury in fact … *as a result of* the fraudulent business practice or false advertising is that a plaintiff actually *relied* on the misrepresentation and as a result, was injured thereby." *See Pfizer Inc. v. Super. Ct.,* 182 Cal. App. 4th 622, 628 (2010) (emphasis in original) (denying class certification because none of the representative plaintiffs "entered into the transaction" as a result of the allegedly misleading advertisements). When the alleged misconduct is a material omission, rather than an affirmative misrepresentation, the plaintiff still must prove reliance. *See e.g., Mirkin v. Wasserman,* 5 Cal. 4th 1082, 1093 (1993) (plaintiff must demonstrate that, had the omitted information been disclosed, plaintiff would have been aware of it and would have acted differently). In this context, "justifiable reliance" is the same as "causation," *i.e.*, the misrepresentation or omission must be an immediate cause of the plaintiff's conduct, absent which the plaintiff would not have entered into the contract or other transaction. *Hall v. Time Inc.*, 158 Cal. App. 4th 847, 855 n.2 (2008).

By their own admissions, the California Plaintiffs Hausauer and Tada cannot prove they relied on anything that Amazon allegedly did or failed to do. Although they had heard of AWS, they had no awareness that AWS provided Capital One's cloud storage. SUMF ¶¶ 53, 55. Neither identified any misrepresentation or omission by AWS, let alone one they relied on. In fact,

precisely the opposite: both expressly acknowledged that Capital One's storage of data in AWS accounts was *not* a factor in their decision to apply for or continue using their Capital One account. SUMF ¶¶ 53 (citing Ex. 53 (Hausauer Tr.) at 228:1–7); SUMF ¶ 55 (citing Ex. 56 (Tada Tr.) at 180:14–18).

Plaintiffs' claims under California's Consumer Legal Remedies Act (CLRA) fail for the same reason. "[T]o bring a CLRA action, not only must a consumer be exposed to an unlawful practice, but some kind of damage must result." *Meyer v. Sprint Spectrum L.P.*, 45 Cal. 4th 634, 641, 645–46 (2009); Cal. Civ. Code § 1780. Additionally, the CLRA proscribes an enumerated list of "unfair methods of competition and unfair or deceptive acts or practices undertaken by any *person in a transaction* intended to result or that results in the sale or lease of goods or services to any consumer." Cal. Civ. Code § 1770 (emphasis added). As shown above, the facts are undisputed that the Plaintiffs were not exposed to any statements or practices by Amazon when they applied for their Capital One accounts, nor did they enter any transaction with Amazon. Finally, as this Court noted in its Order on the motion to dismiss, Plaintiffs' claims fail for the additional reason that they did not provide the statutorily required pre-suit notice to Amazon of their planned CLRA claims.[7] Order at 62 n.30.

Because the facts are undisputed that Hausauer and Tada did not see or rely on any statements by AWS, their UCL and CLRA claims against Amazon fails as a matter of law. *See e.g., Handy v. Logmein, Inc.*, No. 1:14-CV-01355-JLT, 2016 WL 4062102, at *12 (E.D. Cal. Jan.

[7] Although footnote 30 of the Order noted that "Plaintiffs have not, as a matter of law, asserted a cognizable CLRA claim against Amazon," it also stated "[a]s to Count 9 (California Consumer Legal Remedies Act), the Motions are denied." Order at 2. Thus, in an abundance of caution, Amazon moves for summary judgment on the CLRA claims.

27, 2016) (granting summary judgment where plaintiff failed to identify any misrepresentation by defendant).

B. FDUTPA Claim (Count 10): Plaintiffs Cannot Prove that Any Unfair or Deceptive Conduct by AWS Was Likely to Deceive a Reasonable Consumer.

Amazon is entitled to summary judgment on Florida Plaintiffs Zielicke and Behar's Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA") claim because they were not exposed to any misleading statement by Amazon. To prove a FDUTPA violation, Plaintiffs must first establish that something done by Amazon constituted unfair or deceptive conduct likely to deceive a reasonable consumer. *Pop's Pancakes, Inc. v. NuCO2, Inc.*, 251 F.R.D. 677 (S.D. Fla. 2008) (rejecting FDUTPA claim as a matter of law because Plaintiff failed to prove that the fees charged by the defendant were likely to deceive a reasonable consumer); *State v. Commerce Commercial Leasing, LLC*, 946 So. 2d 1253, 1258 (Fla. Dist. Ct. App. 2007) (a FDUTPA plaintiff must show that the defendant "engaged in unconscionable, unfair or deceptive acts or practices likely to deceive a consumer acting reasonably under the circumstances"). Plaintiffs must also prove they suffered actual damages from the unfair and deceptive act. *See In re Crown Auto Dealerships, Inc.,* 187 B.R. 1009, 1018 (Bankr. M.D. Fla. 1995) (plaintiffs entitled to no recovery where they failed to establish actual damages as a result of the alleged misrepresentations).

The facts are undisputed that Zielicke and Behar were not aware of and did not rely on any misrepresentation or deceptive practice by Amazon. Neither had even heard of AWS before this lawsuit. SUMF ¶¶ 50, 58. Both admitted they did not consider Capital One's relationship with AWS when applying for Capital One accounts. *Id*. Accordingly, the Court should grant summary judgment to Amazon on Plaintiffs' FDUTPA claim. *See Ruiz v. Bank of Am., N.A.,* No. 8:17-CV-2586-T-23TGW, 2018 WL 3743529, at *4 (M.D. Fla. Aug. 7, 2018) (granting summary judgment where plaintiff failed to identify a misrepresentation by defendant).

C. New York GBL § 349 Claim (Count 11): Plaintiffs Suffered No Injury Caused by Deceptive Conduct by Amazon.

The Court should grant summary judgment on New York Plaintiff Gershen's claim under New York General Business Law (GBL) section 349 claim because the facts are undisputed that she was not exposed to any misleading statement or practice by Amazon. To prevail on a GBL § 349 claim, "a plaintiff must prove three elements: first, that the challenged act or practice was consumer-oriented; second, that it was misleading in a material way; and third, that the plaintiff suffered injury as a result of the deceptive act." *LaCourte v. JP Morgan Chase & Co.*, 2013 WL 4830935, at *10 (S.D.N.Y. Sept. 4, 2013), *aff'd sub nom. Ritchie v. Taylor*, 701 F.App'x 45 (2d Cir. 2017). "[N]umerous courts have held that in order to have been injured by the defendant's deceptive act, a plaintiff must have been personally misled or deceived." *Id.* at *10 (citing *Solomon v. Bell Atl. Corp.*, 777 N.Y.S.2d 50, 55 (N.Y. App. Div. 2004)). To have been personally misled or deceived, a plaintiff must prove that "he has seen the misleading statements … before he came into possession of the products he purchased." *Oden v. Bos. Sci. Corp.*, 330 F. Supp. 3d 877, 902 (E.D.N.Y. June 4, 2018) (quoting *Goldemberg v. Johnson & Johnson Consumer Cos., Inc.*, 8 F. Supp. 3d 467, 480 (S.D.N.Y. 2014). Summary judgment should be granted for a defendant where the facts are undisputed that the plaintiff was not exposed to a misleading statement or practice. *Douyon v. N.Y. Med. Health Care, P.C.*, 894 F. Supp. 2d 245, 264 (E.D.N.Y. 2012) (granting summary judgment because it was "undisputed that Plaintiff did not receive the … letters containing the allegedly false assertions"), *amended on other grounds*, No. CV 10-3983(AKT), 2013 WL 5423800 (E.D.N.Y Sept. 25, 2013).

The facts are undisputed that Gershen was not exposed to any misleading statement or conduct by Amazon, and therefore could not have suffered injury as a result. Gershen admitted she was not aware of any misrepresentation or omission by Amazon and was not even aware of

AWS as a company before the lawsuit. SUMF ¶ 56. Accordingly, Amazon is entitled to summary judgment on Gershen's GBL § 349 claim.

D. Texas DTPA Claim (Count 12): Plaintiffs Suffered No Injury Caused by Deceptive Conduct by Amazon.

The Court should enter summary judgment for Amazon on Texas Plaintiff Edmondson's Texas Deceptive Trade Practices Act (DTPA) claim because the facts are undisputed that no deceptive acts by Amazon caused her any injury. To prevail on a DTPA claim, a plaintiff must prove that: "(1) the plaintiff is a consumer, (2) the defendant engaged in false, misleading, or deceptive acts, and (3) these acts constitute a producing cause of the consumer's damages." *Gomez v. Wells Fargo Bank, N.A.*, 2010 WL 2900351, at *2 (N.D. Tex. July 21, 2010) (quoting *Doe v. Boys Club of Greater Dallas, Inc.*, 907 S.W.2d 472, 478 (Tex. 1995)).

Even if Edmonson had any evidence that she suffered an injury from the Cyber Incident (there is none), the facts are undisputed that Edmonson did not see or consider any deceptive statements by Amazon when she applied for and used a Capital One account. Edmondson was not even aware of AWS before the lawsuit. SUMF ¶ 51. Edmondson had never seen or relied on any AWS statements, (*see id.* citing Ex. 50 (Edmondson Tr.) at 204:5–13, 204:24–205:4), and consequently AWS's conduct cannot have been a "producing cause" of any damage or injury to Edmondson. *Brown v. Tarbert, LLC*, 616 S.W.3d 159, 167–68 (Tex. App. Ct. 2020) (a "producing cause" is "a substantial factor which brings about the injury and without which the injury would not have occurred"). Accordingly, Amazon is entitled to summary judgment on Plaintiffs' Texas DTPA claim.

E. Virginia Personal Information Breach Notification Act and Washington Data Breach Notice Act Claims (Counts 13 and 14): The Notification Statutes Are Inapplicable Because Amazon Does Not Maintain Plaintiffs' Data and Was Notified of the Cyber Incident by Capital One.

Amazon is entitled to summary judgment on these statutory claims because: (1) the breach notification statutes do not apply to Amazon when AWS did not receive, use, have access to, or "maintain" the consumer data at issue, and (2) even assuming Amazon fell under the purview of these statutes, Plaintiffs cannot establish the requisite elements to prove their claims.

Virginia's and Washington's breach-notification statutes provide that an entity that "maintains" consumer data containing "personal information" must timely notify the owner of the information of any breach that compromises the security of the personal information. *See* Va. Code Ann. § 18.2-186.6 (D); Wash. Rev. Code § 19.255.010 (1).[8] It is well settled that courts are bound by the plain meaning of the language of a statute "unless the terms are ambiguous or applying the plain language would lead to an absurd result." *Taylor v. Commonwealth*, 837 S.E.2d 674, 676–77 (Va. 2020). Here, as neither statute defines the term "maintains," the Court must construe the statutory language to give effect to the legislature's intent, where "[t]hat intent is usually self-evident from the words used in the statute." *Jones v. Commonwealth ex rel. Von Moll*, 502, 814 S.E.2d 192, 194 (Va. 2018); *see also Hubbard v. Henrico Ltd. P'ship,* 497 S.E.2d 335, 338 (Va. 1998) ("When, as here, a statute contains no express definition of a term, the general rule of statutory construction is to infer the legislature's intent from the plain meaning of the language used.").

[8] Virginia's breach notification statute places the burden on the entity that "maintains computerized data" to notify the owner of the information of any breach "without unreasonable delay following discovery of the breach." Va. Code Ann. § 182.186.6 (D). Its counterpart in Washington requires a business that "owns or licenses data that includes personal information" or "maintains data that may include personal information" to provide notice "immediately following discovery." Wash. Rev. Code § 19.255.010 (1)-(2) (2015).

As an initial matter, these statutes cannot apply to Amazon because they require only the entity that "maintains" personal data to notify individuals whose personal information was subject to a breach. Here, it is undisputed that [redacted] SUMF ¶ 10 (citing Ex. 26 (Schmidt Tr.)) at 132:9–14; *see also id.* (citing Ex. 24 (Haken, AWS 30(b)(6) Tr.)) at 129:9–24 (stating that AWS has "built our infrastructure so that we cannot access a guest operating system of our customers' virtual machines"). In other words, AWS, by design, cannot know what type of data is stored in its customers' virtual machines, which contains the customers' own sensitive and proprietary information. *See id.* (citing Ex. 25 (Schuster, AWS 30(b)(6) Tr.)) at 54:1–9 ("Our customers do not want us understanding and knowing the type of data that they're putting into our environment."). Indeed, the Contracts between Capital One and AWS [redacted] *See* SUMF ¶ 4. The agreement further clarifies that [redacted] *See id.* at ¶ 4.4.

Plaintiffs cannot prove that AWS "maintains" the exfiltrated PII as contemplated by the plain language of the Virginia and Washington breach notification statutes. The breach notification statutes are not intended to impose a notification duty on third-party service providers with *no* access or visibility into the consumer subject to a breach. Plaintiffs cannot show any evidence or legal authority to the contrary.

[9] End Users, in this case Capital One's employees and customers, are defined as, "any individual or entity that directly or indirectly through another user: (a) accesses or uses Customer Content; or (b) otherwise accesses or uses the Service Offerings under a Customer account." *See* Ex. 32 (2019 Enterprise Agreement) at 30.

Even assuming *arguendo* that the statutes apply to Amazon, Plaintiffs cannot carry their burden to prove the elements of their claims. First, Plaintiffs have no evidence of notice being unreasonably delayed. Second, [redacted] SUMF ¶ 34 (citing Ex. 26 (Schmidt Tr.) at 61:24–62:2 [redacted]

Finally, as set forth in Section V.A. of Capital One's Motion for Summary Judgment, neither of the two Representative Plaintiffs from Virginia and Washington had their "personal information" compromised as defined by the statute, nor have Plaintiffs identified any damages attributable to allegedly delayed notification. *See also Corona v. Sony Pictures Entm't, Inc.*, 2015 WL 3916744, at *8 (C.D. Cal. June 15, 2015) (dismissing Virginia Personal Information Breach Notification Act claim where "Plaintiffs have failed to plausibly allege any injury resulting from [Defendant]'s alleged untimely notification"); *Grigsby v. Valve Corp.*, 2013 WL 12310666, at *5 (W.D. Wash. Mar. 18, 2013) (dismissing Washington Data Breach Notice Act claim where Plaintiff failed to "allege facts supporting the claim that he was injured due to the interval between the hacking incident and [Defendant]'s notice of the incident and not just that he was injured by the hacking incident alone").

The Court should thus grant summary judgment on the Virginia and Washington notification claims against Amazon.

F. Washington Consumer Protection Act Claim (Count 15): Amazon Did Not Commit a Deceptive Act on Which Plaintiffs Relied to Their Detriment.

Amazon is entitled to summary judgment on Washington Plaintiff Sharp's Washington Consumer Protection Act (WCPA) claim because there is no causal link between her alleged injuries and any deceptive practice by Amazon. To prevail on a WCPA claim, a Plaintiff "must

show (1) an unfair or deceptive act or practice, (2) that occurs in trade or commerce, (3) a public interest, (4) injury to the plaintiff in his or her business or property, and (5) a causal link between the unfair or deceptive act and the injury suffered." *Indoor Billboard/Wash., Inc. v. Integra Telecom of Wash., Inc.*, 162 Wash. 2d 59, 73 (2007). To establish causation, a Plaintiff "would have to establish that but for [AWS's] unfair or deceptive act or practice, [Sharp]'s injury would not have occurred." *Indoor Billboard/Wash., Inc.*, 162 Wash. 2d at 82 Like other states' consumer protection statutes, "Washington requires a private [W]CPA plaintiff to establish the deceptive act caused injury." *Panag v. Farmers Ins. Co. of Wash.*, 166 Wash. 2d 27, 57 (2009).

Amazon could not have caused any injury to Sharp, because the facts are undisputed that she was not exposed to any allegedly deceptive practice or statement by Amazon. To the contrary, Sharp had never heard of AWS before this lawsuit and could not identify any statement by AWS or about AWS. SUMF ¶ 54. She therefore could not have been exposed to and did not rely on any statements by AWS when applying for and using a Capital One account. *See Marts v. U.S. Bank Nat. Assoc.*, 166 F. Supp. 3d 1204, 1209–10 (W.D. Wash. Feb. 26, 2016) (granting motion for summary judgment on WCPA claim where plaintiffs failed to produce sufficient evidence to support their "speculation" that defendants engaged in a deceptive act), *aff'd*, 714 F. App'x 775 (9th Cir. 2018). Accordingly, the Court should grant summary judgment for Amazon on Plaintiffs' WCPA claim.

IV. AMAZON IS ENTITLED TO SUMMARY JUDGMENT ON PLAINTIFFS' DECLARATORY JUDGMENT CLAIM AND REQUEST FOR INJUNCTIVE RELIEF (COUNT 4).

Declaratory relief is appropriate only when it "will serve a useful purpose in clarifying and settling the legal relations in issue, and … when it will terminate and afford relief from the uncertainty, insecurity, and controversy giving rise to the proceeding. It should not be used to try a controversy by piecemeal, or to try particular issues without settling the entire controversy."

Centennial Life Ins. Co. v. Poston, 88 F.3d 255, 256–57 (4th Cir. 1996) (internal citation and quotations omitted). Because Plaintiffs' declaratory relief claim is derivative of their substantive claims, Amazon is entitled to summary judgment for the same reasons described above. Plaintiffs base both their negligence and declaratory judgment claims upon AWS's alleged breach of a "a legal duty to secure consumers' PII." Compl. ¶ 197(a)–(b). The declaratory judgment that Plaintiffs seek adds nothing to clarify or settle the negligence claim. *See Paden v. J.P. Morgan Chase Bank, N.A.*, No. 1:11CV731, 2011 WL 13234307, at *3 (E.D. Va. Nov. 23, 2011) (dismissing declaratory judgment claim where it was "wholly duplicative" of underlying claim) and *Thunander v. Uponor, Inc.*, 887 F. Supp. 2d 850, 878 (D. Minn. 2012) (dismissing declaratory judgment claim in part because it "duplicates the allegations that Plaintiffs allege in essentially all of their claims."). Finally, Plaintiffs' request that the court issue prospective injunctive relief to "employ adequate security practices consistent with law and industry standards to protect consumers PII" (Compl. ¶ 199) fails because, as discussed above, Plaintiffs have not identified any industry standard or what practices would comply with that standard. *See* Madnick Daubert Mot. § II. Nor have Plaintiffs identified any security vulnerabilities in AWS. *Id.*

CONCLUSION

For the reasons stated above, Amazon is entitled to summary judgment on all of Plaintiffs' remaining claims.

Dated: July 2, 2021

Respectfully submitted,

/s/ Robert R. Vieth

Robert R. Vieth, Esq. (VSB No. 24304)
HIRSCHLER FLEISCHER, PC
8270 Greensboro Drive, Suite 700
Tysons Corner, VA 22102
T: (703) 584-8366
F: (703) 584-8901
Email: rvieth@hirschlerlaw.com

Local counsel for Defendants Amazon.com, Inc. and Amazon Web Services, Inc.

Tyler G. Newby (admitted *pro hac vice*)
Laurence F. Pulgram (admitted *pro hac vice*)
Jedediah Wakefield (admitted *pro hac vice*)
Vincent Barredo (admitted *pro hac vice*)
Andrew M. Lewis (admitted *pro hac vice*)
Janie Y. Miller (admitted *pro hac vice*)
Meghan E. Fenzel (admitted *pro hac vice*)
Sarah V. Lightstone (admitted *pro hac vice*)
Rina Plotkin (admitted *pro hac vice*)
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: (415) 875-2300
Facsimile: (415) 281-1350
Email: tnewby@fenwick.com
lpulgram@fenwick.com
jwakefield@fenwick.com
vbarredo@fenwick.com
alewis@fenwick.com
jmiller@fenwick.com
mfenzel@fenwick.com
slightstone@fenwick.com
rplotkin@fenwick.com

Counsel for Defendants Amazon.com, Inc. and Amazon Web Services, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on July 2, 2021, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ Robert R. Vieth
Robert R. Vieth, Esq. (VSB No. 24304)
HIRSCHLER FLEISCHER, PC
8270 Greensboro Drive, Suite 700
Tysons, Virginia 22102
T: (703) 584-8366
F: (703) 584-8901
Email: rvieth@hirschlerlaw.com

CERTIFICATE OF SERVICE

I hereby certify that on July 2, 2021, I caused the foregoing document to be served upon Plaintiffs' Lead Counsel and Local Counsel via electronic mail addressed as follows:

Norman E. Siegel
Jillian R. Dent
Stephanie Walters
Michelle Campbell
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel: (816) 714-7100
siegel@stuevesiegel.com
dent@stuevesiegel.com
walters@stuevesiegel.com
campbell@stuevesiegel.com

Karen Hanson Riebel
LOCKRIDGE GRINDAL NAUN, P.L.L.P.
100 Washington Avenue South, Suite 200
Minneapolis, MN 55401
Tel: (612) 339-6900
khriebel@locklaw.com

John A. Yanchunis
Patrick A. Barthle
MORGAN & MORGAN COMPLEX LITIGATION GROUP
210 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
jyanchunis@ForThePeople.com
pbarthle@forthepeople.com

Steven T. Webster
WEBSTER BOOK LLP
300 N. Washington Street, Suite 404
Alexandria, Virginia 22314
Tel: (888) 987-9991
swebster@websterbook.com

And upon Defendants' Lead Counsel and Local Counsel via electronic mail addressed as follows:

David L. Balser
S. Stewart Haskins II
John C. Toro
Kevin J. O'Brien
Robert D. Griest
KING & SPALDING LLP
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
Tel.: (404) 572-4600
Fax: (404) 572-5140
dbalser@kslaw.com
shaskins@kslaw.com
jtoro@kslaw.com
kobrien@kslaw.com
rgriest@kslaw.com

Robert A. Angle
Tim St. George
Jon S. Hubbard
Harrison Scott Kelly
TROUTMAN SANDERS LLP
1001 Haxall Point
Richmond, VA 23219
Telephone: (804) 697-1200
Facsimile: (804) 697-1339
robert.angle@troutman.com
jon.hubbard@troutman.com
scott.kelly@troutman.com
timothy.st.george@troutman.com

Mary C. Zinsner (VSB No. 31397)
TROUTMAN SANDERS LLP
401 9th Street, NW, Suite 1000
Washington, DC 20004
Telephone: (202) 274-1932
Facsimile: (703) 448-6514
mary.zinsner@troutman.com

/s/ Robert R. Vieth
Robert R. Vieth, Esq. (VSB No. 24304)
HIRSCHLER FLEISCHER, PC
8270 Greensboro Drive, Suite 700
Tysons, Virginia 22102
T: (703) 584-8366
F: (703) 584-8901
Email: rvieth@hf-law.com